

Final Paper

Brandon Rollinson Jr.

August 9, 2026

Employer: Marcos Malvido

Company: CyberQRT

CYSE 368/Internship

Summer 2026

Introduction and Internship Overview

My internship with CyberQRT during Summer 2026 gave me the opportunity to strengthen my cybersecurity knowledge while developing research, writing, analytical, and professional skills. The experience was structured around several stages of work that built on one another. Early in the internship, I focused on reading cybersecurity research papers, taking detailed notes, creating annotated bibliographies, and preparing for the CompTIA Security+ certification. As the internship continued, I began reviewing help desk documentation and identifying ways to improve its clarity and organization. Later, my work shifted toward artificial intelligence and machine learning research and understanding how those technologies can be applied to cybersecurity problems. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

The internship helped me understand that cybersecurity work is not limited to directly configuring systems or responding to attacks. Research, documentation, communication, and continuous learning are also important parts of the field. Many of my assignments required me to read technical material, identify the most important information, and explain complicated ideas in a clear way. This strengthened my ability to think critically instead of only memorizing cybersecurity terminology. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

One of the most valuable parts of the experience was seeing my responsibilities develop over time. The first stage created a foundation in cybersecurity research and Security+ concepts. The next stage introduced documentation review and professional communication. The final stage expanded into AI and machine learning research with the goal of applying what I learned to a cybersecurity-related project. Each stage challenged me in a different way and helped me become more comfortable learning unfamiliar technical concepts. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Overall, my CyberQRT internship supported both my academic and career development. It allowed me to connect concepts from my cybersecurity education to professional research and technical work. It also showed me areas where I have grown and areas where I want to continue improving as I prepare for future opportunities in cybersecurity. Throughout this experience, I also developed stronger

problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Cybersecurity Research and Technical Analysis

A major responsibility throughout my internship was conducting cybersecurity research. I spent significant time reading peer reviewed papers and technical material and taking detailed notes on the information presented. In the beginning, some of the research was challenging because academic papers often use advanced terminology, technical methods, and detailed explanations of experiments. I learned to slow down, identify the research objective, examine the methodology, and focus on the results instead of trying to understand every sentence at once. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

As I gained more experience, I became better at recognizing the structure of research papers and determining which information was most important. I focused on questions such as what problem the researchers were trying to solve, what approach they used, what data supported the experiment, and how they measured success. This process strengthened my analytical skills because I had to evaluate the information rather than simply read it. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

I also created annotated bibliographies that summarized the purpose, findings, and value of research sources. This assignment improved my technical writing because I had to take complicated information and explain it in a more organized and understandable format. It also reinforced the importance of using credible sources when researching cybersecurity topics. Learning to evaluate sources will be useful in future classes, professional projects, and any role that requires me to make decisions based on technical information. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Research became one of the strongest themes of my internship. It taught me that cybersecurity professionals must continue learning because technologies, threats, and defensive methods constantly change. The ability to locate credible information, understand technical evidence, and communicate findings clearly is a skill I expect to use throughout my career. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Security+ Preparation and Cybersecurity Foundations

Another important part of my internship was preparing for the CompTIA Security+ certification. I used internship time to review cybersecurity concepts, study technical material, and complete practice exams. My studying covered areas such as network security, access control, risk management, threats and vulnerabilities, and security operations. Reviewing these subjects helped reinforce concepts that are important for understanding how organizations protect systems, networks, users, and information. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Practice exams were especially useful because they showed me which topics I understood and which areas needed more attention. I learned that success in cybersecurity requires more than memorizing definitions. Many security questions require understanding a scenario, identifying the risk, and choosing the most appropriate control or response. This helped me develop a more practical way of thinking about cybersecurity concepts. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Studying for Security+ also improved my discipline and study habits. Cybersecurity contains a large amount of terminology, technologies, frameworks, and attack methods, so I had to organize the material and repeatedly review weaker areas. The process increased my confidence and helped me connect concepts from my coursework to broader industry knowledge. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These

habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

This stage of the internship reinforced the importance of continuous professional development. Certifications are only one part of building a cybersecurity career, but preparing for Security+ encouraged me to build a stronger technical foundation. That foundation supported the research and AI related work I completed later in the internship because I had a better understanding of the security problems that new technologies are designed to address. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Help Desk Documentation Review

As the internship progressed, my responsibilities shifted toward reviewing help desk documentation. My assignment was to examine the help desk file set, take detailed notes, and identify areas that could be improved. I looked for instructions that could be explained more clearly, information that might confuse a reader, and sections that overlapped with other documents. I also considered whether repeated information could be condensed so that the documentation would be easier to maintain and use. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

This work showed me how important documentation is in a technical environment. Even when the technical solution to a problem is correct, poorly written instructions can slow down employees or cause inconsistent results. Clear documentation allows users and support personnel to follow the same process and reduces the amount of time spent trying to determine what a document means. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

The documentation review also strengthened my attention to detail. I had to look at the material from the perspective of someone who might be using the instructions for the first time. That required me to think about whether steps were complete, whether wording was understandable, and whether information was organized logically. I learned that technical writing should be accurate but also practical for the intended audience. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical

documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

This responsibility expanded my understanding of cybersecurity and IT operations because secure and reliable systems depend on repeatable processes. Documentation supports troubleshooting, training, communication, and consistency. The assignment helped me see that improving technical documentation can contribute to a more efficient organization and can support better security practices by making procedures easier to follow. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Artificial Intelligence and Machine Learning Research

Later in the internship, my primary focus became artificial intelligence and machine learning. I researched how these technologies work and how they are being applied within cybersecurity. I reviewed peer reviewed papers, technical articles, and other industry material while taking detailed notes. My goal was to understand both the basic concepts behind machine learning and the practical ways AI can support cybersecurity operations. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

I studied supervised, unsupervised, and reinforcement learning and learned that different approaches are appropriate for different types of problems. I also reviewed concepts such as neural networks, deep learning, feature engineering, training data, and model evaluation. This helped me understand that a machine learning model depends on more than the algorithm itself. The quality of the dataset, preprocessing, feature selection, training process, and evaluation method can significantly affect the results. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

My research also focused on cybersecurity applications. I learned how machine learning can be used to identify malicious network traffic, detect phishing emails, classify malware, recognize insider threats, and identify abnormal user behavior. AI can process large amounts of information quickly, which can help security teams identify patterns and potential threats that would be difficult for an analyst to review manually at the same scale. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I

learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

This stage of the internship was valuable because it connected cybersecurity with an emerging technical area. It helped me understand why AI and machine learning are becoming increasingly important to security operations while also showing me that these technologies must be evaluated carefully before they are trusted in real environments. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Evaluating AI Models and Research Results

While reading AI and machine learning research, I focused on more than the final accuracy reported by a paper. I examined the researchers' objectives, methods, datasets, and evaluation process. I compared approaches and looked at why one model might perform better than another. This helped me become more critical when reading technical claims because a strong result is meaningful only when the experiment and evaluation process support it. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

I learned about common evaluation metrics including accuracy, precision, recall, and F1 score. These metrics helped me understand how researchers determine whether a model is performing effectively. A model may appear successful based on one measurement while still having weaknesses that become clearer when additional metrics are considered. Learning these concepts improved my ability to interpret the results presented in research papers. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

My internship research also emphasized finding recent peer reviewed work, including papers from 2025 and 2026, that could potentially be reproduced. Important factors included the availability of public datasets, enough information about the experiment, and sufficient performance metrics to compare results. Thinking about reproducibility made the research feel more practical because the goal was not

only to read about a model but to determine whether its approach could become the foundation for future project work. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Working through technical papers sometimes required rereading sections and researching unfamiliar concepts. Although this was challenging, it improved my ability to break down complex information. Over time, I became more comfortable with common machine learning terminology and with evaluating how researchers designed and tested their models. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Transition from Research to Project Development

The later stage of my internship introduced the next step of turning research into a practical project. After spending time studying AI and machine learning, the goal was to begin creating a project based on the concepts I had learned. This transition was important because it moved the experience from understanding existing research toward thinking about how an AI or machine learning approach could be applied to a cybersecurity-related problem. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Planning this type of project requires several connected decisions. The process includes identifying an appropriate problem, selecting a useful dataset, preparing the data, choosing a machine learning model, evaluating the model's performance, and improving the approach based on the results. My research helped me understand why each of these stages matters and why a successful project cannot depend on the model alone. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

The project-development phase also showed me the relationship between research and implementation. Research provides evidence about methods that have already been tested, while development requires applying those ideas under a specific set of conditions. A project may require adjustments depending on the dataset, goals, available resources, and performance requirements. This encouraged me to think more like a problem solver rather than only a reader of technical information. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

I was especially interested in this transition because practical development can reinforce concepts that are difficult to fully understand through reading alone. Applying the research gives me an opportunity to see how data preparation, model selection, and evaluation work together. It also provides a way to connect AI research directly to cybersecurity challenges. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Professional Development, Communication, and Challenges

The internship contributed to my professional growth in addition to my technical development. One change during the experience was the introduction of daily progress meetings with my supervisor. These check ins were designed to review progress, discuss challenges, and plan upcoming work. Communicating about my assignments helped me understand the importance of keeping others informed and being prepared to explain what I had completed and what I needed to do next. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

The meetings also supported organization and time management. When working on research, it can be easy to spend too much time on one paper or one difficult concept. Having regular progress discussions encouraged me to think about priorities and measurable progress. Feedback is also important because it can identify issues before too much time is spent moving in the wrong direction. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing

conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

One challenge during the internship was that physical cybersecurity kit training was delayed while additional equipment was being obtained. Instead of allowing the delay to stop my progress, the internship shifted attention toward documentation review and research. This showed me that professional work does not always follow the original schedule and that it is important to remain productive when plans change. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Another challenge was learning technical AI and machine learning concepts that were unfamiliar to me. Some papers required additional reading and repeated review. Working through that difficulty increased my confidence in my ability to learn complex material. I learned that I do not need to immediately understand every concept; I need a process for researching, taking notes, asking questions, and continuing until the material becomes clearer. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Overall Reflection and Career Impact

Looking back on my CyberQRT internship, I can see clear growth from the beginning of the experience to the final stage. I started by building my cybersecurity foundation through research, annotated bibliographies, and Security+ preparation. I then gained experience reviewing professional documentation and thinking about how technical information can be improved for the people who use it. Finally, I expanded into AI and machine learning research and began preparing to apply that knowledge through project development. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

The experience strengthened several skills that I will continue to use in cybersecurity. My research skills improved because I learned how to approach technical papers and identify their most important elements. My analytical skills improved because I had to compare methods, datasets, and results. My writing skills improved through note taking, annotated bibliographies, documentation review, and explaining technical concepts. I also developed professionally through progress meetings, changing assignments, and managing work across different areas. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing

through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

The internship reinforced the importance of continuous learning. Cybersecurity changes quickly, and artificial intelligence is adding new opportunities and challenges to the field. Security professionals need to understand current threats while also staying aware of technologies that may change how attacks are performed and how organizations defend themselves. My experience researching AI applications in threat detection, phishing identification, malware classification, and abnormal behavior analysis gave me a stronger understanding of this direction. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.

Overall, CyberQRT provided an experience that supported my education and future career goals. It gave me the opportunity to build knowledge through research while also developing the professional habits needed to work on technical assignments. I am leaving the internship with stronger confidence in my ability to learn unfamiliar subjects, analyze technical information, communicate my findings, and continue developing as a cybersecurity professional. Throughout this experience, I also developed stronger problem solving skills by approaching each assignment methodically. Rather than rushing through technical material, I learned to break complex topics into smaller sections, research unfamiliar concepts, and connect new information to knowledge I had already gained from my coursework. This approach made it easier to understand advanced cybersecurity concepts and improved my confidence when working with technical documentation. I also became more comfortable asking questions, reviewing multiple sources, and validating information before drawing conclusions. These habits are essential in cybersecurity because accurate analysis and careful attention to detail often determine the quality of technical decisions and recommendations.